

AO 91 (Rev 11/11) Criminal Complaint

UNITED STATES DISTRICT COURT

for the

Eastern District of Pennsylvania

United States of America)

v.)

Sean Christopher Williams)

Case No. 19-493-M

[UNDER SEAL]

Defendant(s)

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of March 2014 to November 2014 in the county of Montgomery in the
Eastern District of Pennsylvania, the defendant(s) violated:

<i>Code Section</i>	<i>Offense Description</i>
18 U.S.C. § 1344	bank fraud
18 U.S.C. § 1343	wire fraud
18 U.S.C. § 1028A	aggravated identity theft

This criminal complaint is based on these facts:

See attached Affidavit.

☒ Continued on the attached sheet.


Complainant's signature

Lorelei Rae Schreier, Special Agent, FBI

Printed name and title

Sworn to before me and signed in my presence.

Date: 03/26/2019


Judge's signature

City and state: Philadelphia, Pennsylvania

Honorable Timothy R. Rice, U.S. Magistrate Judge

Printed name and title

AFFIDAVIT

I, Lorelei Rae Schreier, depose and swear as follows:

Background of the Affiant

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI") and have been so employed since July 2010. I am currently assigned to the Philadelphia Field Office, Fort Washington Resident Agency, where I investigate crimes including investment fraud, financial institution fraud, mortgage fraud, corporate fraud, and computer crime, among others. I have received extensive training from the FBI and other government agencies in various mail and wire fraud violations.

2. As a federal agent, I am authorized to investigate violations of the laws of the United States and to execute warrants issued under the authority of the United States.

Purpose of the Affidavit

3. As explained in detail below, I have probable cause to believe that SEAN CHRISTOPHER WILLIAMS ("WILLIAMS") committed, within the Eastern District of Pennsylvania and elsewhere, violations of 18 U.S.C. §§ 1028A, 1343, and 1344. As described in detail below, there is probable cause to believe that WILLIAMS perpetrated a scheme whereby he would establish fraudulent bank accounts at different financial institutions in the name of his victim. Then, WILLIAMS would effect a transfer of funds from one of the fraudulent accounts to another. Then, WILLIAMS would use the fraudulently obtained funds to pay his student loans, credit card debt, or other personal obligations. WILLIAMS would effect these transactions before the banks were able to determine that the accounts were fraudulent and that no actual funds existed to cover the transfers.

4. I submit this affidavit in support of a criminal complaint and arrest warrant for WILLIAMS for: (a) bank fraud, in violation of 18 U.S.C. § 1344; (b) wire fraud, in violation of 18 U.S.C. § 1343; and (c) aggravated identity theft, in violation of 18 U.S.C. § 1028A.

5. For the reasons set forth herein, there is probable cause to believe that, from at least in or around March 2014 to at least in or around November 2014, WILLIAMS, in the Eastern District of Pennsylvania and elsewhere:

- a. knowingly executed, and attempted to execute, a scheme to defraud Ally Bank (certificate no. 57803) and The Huntington National Bank (certificate no. 6560), each of which is a financial institution with deposits insured by the Federal Deposit Insurance Corporation, and to obtain monies owned by and under the care, custody, and control of each bank by means of false and fraudulent pretenses, representations, and promises, in violation of 18 U.S.C. § 1344;
- b. devised and intended to devise a scheme to defraud and to obtain money and property by means of false and fraudulent pretenses, representations, and promises, in violation of 18 U.S.C. § 1343; and
- c. knowingly and without lawful authority used a means of identification of another person, that is the name and social security number of J.S. (whose full name and social security number are known to Your Affiant), during and in relation to bank fraud and wire fraud, in violation of 18 U.S.C. § 1028A.

6. The information contained in this affidavit is based upon, among other things: my personal knowledge, my general experience in identity theft and fraud investigations, information provided to me by other law enforcement officers, information provided to me by the victims of this fraud, and my review of documents.

7. This affidavit is being executed as part of an ongoing investigation and is based on my current understanding of the relevant facts. As the investigation proceeds, new facts may come to light that qualify or contradict prior facts. Because this affidavit is being

submitted for the limited purpose of establishing probable cause for the criminal complaint and arrest warrant, Your Affiant has not included each and every fact known concerning this investigation. Rather, the facts set forth herein constitute a summary of the investigation and the known facts. Further, Your Affiant has only set forth the facts that Your Affiant believes are necessary to establish probable cause to believe that WILLIAMS has violated (a) 18 U.S.C. § 1344; (b) 18 U.S.C. § 1343; and (c) 18 U.S.C. § 1028A.

Applicable Laws

8. Title 18, United States Code, Section 1344 makes it unlawful to:

knowingly execute[], or attempt[] to execute, a scheme or artifice—

- (1) to defraud a financial institution; or
- (2) to obtain any of the moneys, funds, credits, assets, securities, or other property owned by, or under the custody or control of, a financial institution, by means of false or fraudulent pretenses, representations, or promises[.]

9. Title 18, United States Code, Section 1343 makes it unlawful to:

having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmit[] or cause[] to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, and writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice[.]

10. Title 18, United States Code, Section 1028A(a)(1) states: “Whoever, during and in relation to any felony violation enumerated in subsection (c), knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person shall, in addition to the punishment provided for such felony, be sentenced to a term of imprisonment of 2 years.” Title 18, United States Code, Section 1028A(c)(5) states that, “[f]or purposes of this

section, the term ‘felony violation enumerated in subsection (c)’ means any offense that is a felony violation of . . . any provision contained in chapter 63 (relating to mail, bank, and wire fraud).” A violation of 18 U.S.C. § 1344 is punishable by a fine, imprisonment of not more than thirty years, or both, and a violation of 18 U.S.C. § 1343, which affects a financial institution, is punishable by a fine, imprisonment of not more than thirty years, or both. Thus, such violations are felonies. See 18 U.S.C. § 3559(a)(2) (classifying an offense with a maximum term of imprisonment of twenty-five years or more as a “Class B felony”).

Summary of the Investigation

11. Based on my review of public source documents and records obtained through subpoenas, WILLIAMS was born on [redacted], 1981, and currently resides at 5304 The Valley, N.E., Sandy Springs, Georgia.¹

12. Based on my conversations with bank employees and my review of a Federal Deposit Insurance Corporation (“FDIC”) database, at all relevant times Ally Bank (“Ally”) was a financial institution located in Fort Washington, Pennsylvania, the deposits of which were insured by the FDIC, certificate number 57803. Ally is an Internet bank; that is, a bank which does not have physical branch locations in the way a traditional bank does, but which operates over the Internet. Customers open checking accounts and savings accounts, and conduct other routine banking business, but do so over the Internet rather than by visiting a bank branch.

13. Based on my conversation with a representative of Ally, at all relevant times all requests for the transfer of funds into or out of an Ally bank account—whether that request is made by telephone or online—were processed by Ally’s Operations Center in Fort

¹ Full birth date known to Your Affiant but redacted here.

Washington, Pennsylvania, which is in the Eastern District of Pennsylvania. Wire transfers were, at all relevant times, processed electronically from Ally's Fort Washington Operations Center. For funds that were transferred into Ally, Ally's Fort Washington Operations Center receives the funds electronically and then electronically initiates the deposit into the Ally customer account.

14. Based on my conversations with bank employees and my review of an FDIC database, The Huntington National Bank ("HNB") has its headquarters in Ohio and physical banking locations throughout Florida, Illinois, Indiana, Kentucky, Michigan, Ohio, Pennsylvania, West Virginia, and Wisconsin. In addition, and like Ally, HNB customers can open checking accounts and savings accounts, and conduct routine banking business, over the Internet. Deposits at HNB are, and at all relevant times were, insured by the FDIC, certificate number 6560.

15. Based on my interviews with bank employees and my review of Ally records, from in or about March 2014 to in or about November 2014, Ally learned that at least fifty-one suspected fraudulent bank accounts created online at Ally were linked by customer online application data. Ally first learned of this suspected fraud in November 2014 when HNB contacted Ally to inform Ally that a number of HNB's customers had received notifications of fraudulent charges and withdrawals on accounts that they had not opened. HNB traced the deposited funds to accounts held at Ally.

16. Based on my interviews with bank employees, Ally's internal investigation revealed that, in 2010, a customer identified as WILLIAMS, opened an account with Ally. Ally determined that it had closed one of WILLIAMS's accounts in 2012, after it was

used to conduct unauthorized business transactions. Through diagnostic analytics, Ally linked WILLIAMS's online Ally accounts to the suspected fraudulent victim accounts.

17. Through a search warrant, the FBI obtained the Internet Protocol (or "IP") addresses used to open the fifty-one suspected fraudulent accounts at Ally. For at least certain of the relevant periods, the IP addresses were associated with 27505 Franklin Road, in Southfield, Michigan, the location of an apartment complex in which WILLIAMS was residing at the time. Driver license records, online database searches, credit card records, student loan records, brokerage records, and cable television invoices show that WILLIAMS was residing at that address.²

18. Through a search warrant, Your Affiant obtained records from BeenVerified, Inc. ("BeenVerified"), which indicate a credit card in the name of WILLIAMS was used for transactions with BeenVerified. Specifically, the records show that payment was effected through a credit card in WILLIAMS's name. BeenVerified is an online search tool, whereby users can obtain personal and identifying information about individuals. Records obtained through the search warrant show that, for forty-nine of the fifty-one identity fraud victims at Ally, the account linked to the WILLIAMS's credit card performed research on the individuals immediately before the opening of the suspected fraudulent bank accounts matching these same identities.

19. By comparing the list of fraudulent bank accounts from Ally with customer complaints from other victims at HNB, the FBI determined that the fraudulent Ally accounts were created in the same names as the victim accounts at HNB. The fraudulent Ally accounts were then used to request and to accept incoming funds from bank accounts at HNB.

² The IP addresses were associated with the location of the apartment complex, not WILLIAMS's particular unit.

Through financial analysis, the FBI found that the stolen funds were subsequently transferred out of Ally to pay debts in WILLIAMS's name. One example of the fifty-one occurrences is as follows:

- a. Based on my review of records, including the return from the BeenVerified search warrant, on or about April 18, 2014, the BeenVerified account associated with the WILLIAMS credit card performed a "person report" on a J.S. (J.S.'s name is known to Your Affiant, but is redacted here), which provided information about J.S.'s existence and identity, including the month and year of J.S.'s date of birth.
- b. Based on my review of records, on or about April 18, 2014, a device linked to an IP address associated with the apartment complex discussed in Paragraph 17, above, created fraudulent accounts at Ally and HNB, respectively, in J.S.'s name. As part of the processes to set up the accounts at Ally and HNB, respectively, the name and social security number of J.S. (which are known to Your Affiant) were provided to those banks. Subsequently, a device linked to an IP address associated with the apartment complex made an online transaction request for approximately \$18,351 to be transferred from the fraudulent HNB account to the fraudulent Ally account. Then, on or about April 23, 2014, one electronic payment to an American Express charge card in WILLIAMS's name in amount of \$10,451 was made from the fraudulent Ally account. Then, on or about April 24, 2014, three payments to WILLIAMS's personal student loan account in the amounts \$1,282.96, \$3,125.12, and \$2,545.96, respectively, were made from the fraudulent Ally account. And, on or about April 25, 2014, one payment of \$121.74 to WILLIAMS's Chase credit card account and one payment of \$783.34 to WILLIAMS's American Express charge card account were made from the fraudulent Ally account.
- c. Based on my review of records, including the return from the BeenVerified search warrant, on or about May 2, 2014, the BeenVerified account linked to the WILLIAMS credit card performed another "person report" on J.S., which provided information about J.S.'s existence and identity, including the month and year of J.S.'s date of birth.
- d. Based on my review of records, on or about May 2, 2014, a device linked to an IP address associated with the apartment complex discussed in Paragraph 17, above, created another fraudulent Ally

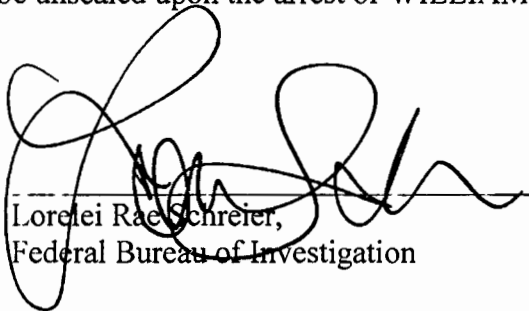
account in J.S.'s name. Then, on or about May 6, 2014, a device linked to an IP address associated with the apartment complex transferred \$15,634 from the previously identified fraudulent HNB account to the second fraudulent Ally account, both of which were in J.S.'s name. On or about May 9, 2014, a transfer of \$15,634 from the second fraudulent Ally account was made to an American Express charge card account in WILLIAMS's name.

- e. Based on my interview with an Ally bank employee, the transactions involving Ally described in subparagraphs 19(b) and 19(d) were processed at Ally's Operations Center in Montgomery County, in the Eastern District of Pennsylvania.

Conclusion and Request for Sealing

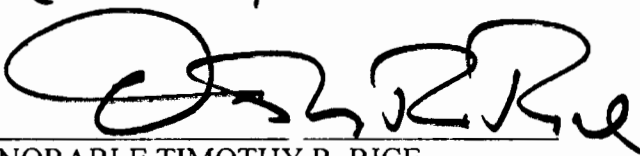
20. Based on the foregoing, there is probable cause to believe that WILLIAMS committed: (a) bank fraud, in violation of 18 U.S.C. § 1344; (b) wire fraud, in violation of 18 U.S.C. § 1343; and (c) aggravated identity theft, in violation of 18 U.S.C. § 1028A.

21. Because this is an application that pertains to an ongoing criminal investigation and because disclosure of the information contained herein as well as disclosure of the warrant being requested herein may compromise the investigation by informing the target of the investigation of the nature and techniques of the investigation, and affording the target of the investigation an opportunity to flee or to destroy or to tamper with evidence or witnesses, Your Affiant requests that the arrest warrant, criminal complaint, and this affidavit, and all related papers, be ordered sealed by the Court, and be unsealed upon the arrest of WILLIAMS or further order of the Court.



Lorelei Rae Schreier,
Federal Bureau of Investigation

Sworn to and subscribed before me this
26 day of March, 2019.



HONORABLE TIMOTHY R. RICE
UNITED STATES MAGISTRATE JUDGE